

## 受領書

平成11年 9月22日

特許庁長官

識別番号 100078868

氏名(名称) 河野 登夫 殿

提出日 平成11年 9月22日

以下の書類を受領しました。

項番	書類名	整理番号	受付番号	出願番号通知(事件の表示)
1	出願審査請求	12928	59900925171	特願平 4-277899
2	特許願	20565	59900925172	特願平11-269407
3	特許願	NEA0991027	59900925176	特願平11-269408
4	意見書	17435	59900925179	特願平 8-316665
5	手続補正書	17435	59900925180	特願平 8-316665
6	意見書	18329	59900925181	特願平 9-223964
7	手続補正書	18329	59900925182	特願平 9-223964
8	特許願	20391	59900925184	特願平11-269409

以 上

BEST AVAILABLE COPY

【書類名】 特許願

【整理番号】 20565

【提出日】 平成11年 9月22日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/14  
H04L 9/30  
G09C 1/00

【発明の名称】 暗号化方法, 暗号通信方法及び暗号文作成装置

【請求項の数】 3

【発明者】

【住所又は居所】 大阪府箕面市栗生外院4丁目15番3号

【氏名】 笠原 正雄

【発明者】

【住所又は居所】 京都府京都市伏見区竹田向代町136番地 村田機械株式会社 本社工場内

【氏名】 村上 恭通

【特許出願人】

【識別番号】 000006297

【氏名又は名称】 村田機械株式会社

【代表者】 村田 純一

【特許出願人】

【識別番号】 597008636

【氏名又は名称】 笠原 正雄

【代理人】

【識別番号】 100078868

【弁理士】

【氏名又は名称】 河野 登夫

【電話番号】 06-6944-4141

【手数料の表示】

11-269407

整理番号＝ 2 0 5 6 5

提出日 平成 1 1 年 9 月 2 2 日  
頁: 2 / 2

【予納台帳番号】 0 0 1 8 8 9

【納付金額】 2 1 0 0 0

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9 8 0 5 2 8 3

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化方法、暗号通信方法及び暗号文作成装置

【特許請求の範囲】

【請求項１】 暗号化すべき平文を分割した分割平文と、該分割平文毎に準備してある複数の公開鍵から任意に選択した公開鍵とを使用して暗号文を作成する暗号化方法において、前記複数の公開鍵として、前記分割平文毎に設定した乱数項が組み込まれた複数の公開鍵を前記分割平文毎に準備しておくことを特徴とする暗号化方法。

【請求項２】 一方のエンティティ側で平文を分割した分割平文と公開鍵とを用いて暗号文を作成して他方のエンティティ側へ伝送し、伝送された暗号文を該他方のエンティティ側で元の平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、前記分割平文毎に設定した乱数項が組み込まれている複数の公開鍵から各分割平文について任意の公開鍵を選択し、選択した公開鍵を使用して暗号文を作成し、作成した暗号文を前記他方のエンティティへ伝送することを特徴とする暗号通信方法。

【請求項３】 暗号化すべき平文を分割した分割平文と公開鍵とを用いて暗号文を作成する装置において、前記分割平文毎に設定した乱数項が組み込まれている複数の公開鍵を予め格納しておく手段と、各分割平文について前記複数の公開鍵から任意の公開鍵を選択する手段と、選択した公開鍵を使用して暗号文を作成する手段とを備えることを特徴とする暗号文作成装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、公開鍵を用いて平文を暗号文に変換する公開鍵暗号系の暗号化方法、この暗号化方法を利用した暗号通信方法、及び、その暗号文を作成する暗号文作成装置に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤と

して、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事、外交面で用いられてきた暗号技術が注目されている。

#### 【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

#### 【０００４】

暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ共通鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を元に平文に復号する。

#### 【０００５】

これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵によって変換された暗号文は秘密鍵でのみ復号することができる。

## 【0006】

## 【発明が解決しようとする課題】

公開鍵暗号系の1つの方式として、積和型暗号方式が知られている。これは、送信者である一方のエンティティ側で平文をK分割した平文ベクトル $m = (m_1, m_2, \dots, m_K)$ と公開鍵である基数ベクトル $c = (c_1, c_2, \dots, c_K)$ とを用いて、暗号文 $C = m_1 c_1 + m_2 c_2 + \dots + m_K c_K$ を作成し、受信者である他方のエンティティ側でその暗号文Cを秘密鍵を用いて平文ベクトルmに復号して元の平文を得る暗号化形式である。

## 【0007】

このような整数環上の演算を利用した積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。そこで、本発明者等は、平文を多進法を用いて表現するようにして、高速な復号処理を可能とした積和型暗号における暗号化方法及び復号方法を提案している（特願平10-262036号，特願平10-262037号）。

## 【0008】

以下、特願平10-262036号に提案した暗号化方法及び復号方法について説明する。秘密鍵と公開鍵とを以下のように準備する。

- ・秘密鍵： $\{b_1\}$ ， $\{v_1\}$ ， $P$ ， $w$
- ・公開鍵： $\{c_1\}$

基数積 $b_1, b_2, \dots, b_i$ に乱数項 $v_1$ を乗じて、基数 $B_1$ を下記(1)のように与える。

$$B_1 = v_1 b_1 b_2 \dots b_i \quad \dots (1)$$

ここで、式(1)で示される各 $B_1$ がほぼ同じ大きさになるように $v_1$ を設定する。但し、 $\gcd(v_1, b_{i+1}) = 1$ を満たすものとする。

## 【0009】

乱数 $w$ を用いて、公開鍵 $\{c_1\}$ を下記(2)のように求める。

$$c_1 \equiv w B_1 \pmod{P} \quad \dots (2)$$

平文をK分割したメッセージ $\{m_1\}$ と公開鍵 $\{c_1\}$ との積和演算により、

下記(3)のように、暗号文Cを得る。

$$C = m_1 c_1 + m_2 c_2 + \dots + m_K c_K \quad \dots (3)$$

【0010】

復号処理は、以下のようにして行われる。

暗号文Cに対して、中間復号文Mを下記(4)のようにして求める。

$$M \equiv w^{-1} C \pmod{P} \quad \dots (4)$$

この中間復号文Mは、具体的には式(5)として与えられるので、以下に示す逐次復号アルゴリズムによって復号できる。

$$M = m_1 b_1 v_1 + m_2 b_1 b_2 v_2 + \dots + m_K b_1 b_2 \dots b_K v_K \quad \dots (5)$$

【0011】

[逐次復号アルゴリズム]

ステップ1

$$M_1 = M / b_1$$

$$m_1 \equiv M_1 v_1^{-1} \pmod{b_2}$$

ステップi (i = 2 ~ K-1)

$$M_i = (M_{i-1} - m_{i-1} v_{i-1}) / b_i$$

$$m_i \equiv M_i v_i^{-1} \pmod{b_{i+1}}$$

ステップK

$$M_K = (M_{K-1} - m_{K-1} v_{K-1}) / b_K$$

$$m_K = M_K / v_K$$

【0012】

元来、このような公開鍵暗号方式は、その安全性の根拠を、因数分解の困難さ、離散対数問題を解くことの困難さに置いており、それに対する攻撃も種々のものが提案されている。

【0013】

本発明は斯かる事情に鑑みてなされたものであり、圧倒的多数の公開鍵の組合せの中から公開鍵の組を自由に選ぶことができる点に安全性の根拠を置いた新しいタイプの公開鍵暗号系の暗号化方法、この暗号化方法を利用した暗号通信方法

、及び、その暗号文を作成する暗号文作成装置を提供することを目的とする。

#### 【００１４】

##### 【課題を解決するための手段】

請求項１に係る暗号化方法は、暗号化すべき平文を分割した分割平文と、該分割平文毎に準備してある複数の公開鍵から任意に選択した公開鍵とを使用して暗号文を作成する暗号化方法において、前記複数の公開鍵として、前記分割平文毎に設定した乱数項が組み込まれた複数の公開鍵を前記分割平文毎に準備しておくことを特徴とする。

#### 【００１５】

請求項２に係る暗号通信方法は、一方のエンティティ側で平文を分割した分割平文と公開鍵とを用いて暗号文を作成して他方のエンティティ側へ伝送し、伝送された暗号文を該他方のエンティティ側で元の平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、前記分割平文毎に設定した乱数項が組み込まれている複数の公開鍵から各分割平文について任意の公開鍵を選択し、選択した公開鍵を使用して暗号文を作成し、作成した暗号文を前記他方のエンティティへ伝送することを特徴とする。

#### 【００１６】

請求項３に係る暗号文作成装置は、暗号化すべき平文を分割した分割平文と公開鍵とを用いて暗号文を作成する装置において、前記分割平文毎に設定した乱数項が組み込まれている複数の公開鍵を予め格納しておく手段と、各分割平文について前記複数の公開鍵から任意の公開鍵を選択する手段と、選択した公開鍵を使用して暗号文を作成する手段とを備えることを特徴とする。

#### 【００１７】

本発明では、平文を分割した分割平文毎に整数と乱数項との積からなる複数の公開鍵が予め準備されており、準備されているそれらの複数の公開鍵から任意の公開鍵を各分割平文毎に選択し、選択した公開鍵を使用して暗号文を作成する。このように本発明では、公開鍵を任意に選択するので、つまり、送信者であるエンティティ側で自由に公開鍵を選択して暗号文を作成するので、その公開鍵の選択パターンが攻撃者には不明であるため、攻撃は困難となる。このように本発明



では、従来例とは異なり、その安全性の根拠を、圧倒的多数の公開鍵の組合せの中から公開鍵の組を自由に選択することに置いている。また、選択するこれらの公開鍵に乱数項を組み込ませるようにしたので、安全性をより高めることができる。

#### 【0018】

##### 【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図1は、本発明による暗号化方式をエンティティA、B間の情報通信に利用した状態を示す模式図である。図1の例では、一方のエンティティA側で、平文xを暗号文Cに暗号化し、通信路1を介してその暗号文Cを他方のエンティティBへ送信し、エンティティB側で、その暗号文Cを元の平文xに復号する場合を示している。

#### 【0019】

送信側であるエンティティAには、平文xを複数の分割平文に分割する平文分割器2と、公開鍵リストを格納するデータベース10から各分割平文に対する公開鍵を選択する公開鍵選択器3と、選択した公開鍵と各分割平文とを用いて暗号文Cを作成する暗号化器4とが備えられている。また、受信側であるエンティティBには、送られてきた暗号文Cを元の平文xに復号する復号器5が備えられている。この例では、公開鍵リストの発行者は受信側のエンティティBであり、その公開鍵リストの利用者は送信側のエンティティAである。

#### 【0020】

次に、具体的な手法について説明する。本発明の基本の暗号化方式は、前述した特願平10-262036号提案の方式（以下、従来方式という）の改良方式である。

#### 【0021】

従来方式に基づく本発明の暗号化方式の初回伝送時における中間復号文Mは、下記（6）で与えられる。

$$M = m_1 \cdot b_1 \cdot v_1 + m_2 \cdot b_1 \cdot b_2 \cdot v_2 + \cdots \\ + m_K \cdot b_1 \cdot b_2 \cdots b_K \cdot v_K \quad \cdots (6)$$

#### 【0022】

但し、 $m_i'$  はメッセージ（分割平文） $m_i$  に対し、 $\log_2 J$  ビットの冗長を付加することにより、与えられた  $j$  について  $J$  を法として、下記（7）が成立するように符号化されている。 $J = 2^g$  の場合、この符号化を非常に単純に実現したい場合には、 $m_i$  を上位に  $g$  桁だけシフトし、下位  $g$  桁に  $j$  を接続すれば良い。即ち、符号化  $m_i'$  は単に  $m_i' = m_i * j$  で与えられる。

$$m_i' \equiv j \pmod{J} \quad \dots (7)$$

#### 【0023】

なお、エンティティ A が選択した公開鍵を用いた一連の暗号文を送り終えるまでの一定期間内で、最初の暗号文以外ではメッセージ  $m_i$  が復号されないことが考えられる。この場合、レートが若干高くなるとともに、復号過程が単純化される。

#### 【0024】

図2は、各分割平文毎に複数の公開鍵を予め格納しているデータベース10内の公開鍵リストを示す図である。図2において、 $K$  は平文  $x$  の分割数（クラス数）を表す。基数積に乱数項を乗じた集合  $\{b_1, b_2, \dots, b_i, v_i^{(j)}\}$  が、図2に示すように、各分割平文毎（各クラス毎）に  $J$  個ずつの公開鍵として準備されている。

#### 【0025】

エンティティ B は、基数積と乱数項とのこれらの積を乱数  $w$  により変換して公開する。即ち、図2に示す基数積と乱数項との積を下記（8）のように変換し、その集合  $\{c_{ij}\}$  を公開する。

$$b_1, b_2, \dots, b_i, v_i^{(j)} w \equiv c_{ij} \pmod{P} \quad \dots (8)$$

#### 【0026】

エンティティ A がランダムに選択した公開鍵の組を下記（9）と表記する。この場合、エンティティ A を含む任意のエンティティにとって、 $J^K$  ( $\gg 1$ ) 通りの公開鍵選択の可能性がある。

#### 【0027】

【数1】

$$(c_1, j_1, c_2, j_2, \dots, c_K, j_K) \dots (9)$$

【0028】

エンティティAは、上記(9)に示す選択した公開鍵の組に基づいて、 $m_i' \equiv j_i \pmod{J}$ とした上で、エンティティBへの暗号文Cを下記(10)のように生成する。

【0029】

【数2】

$$C = m_1' c_{1, j_1} + m_2' c_{2, j_2} + \dots + m_K' c_{K, j_K} \dots (10)$$

【0030】

エンティティBは、このようにして生成される暗号文Cを復号するために、図2における乱数項 $v_i^{(j)}$ を下記(11)のように予め定めておく。但し、 $w_{b, i}$ ,  $r_i^{(j)}$ は何れも乱数である。

$$v_i^{(j)} = w_{b, i} + r_i^{(j)} b_{i+1} \dots (11)$$

【0031】

更にエンティティBは、下記(12)を満たす $w_{b, i}^{-1}$ を秘密鍵として保持する。

$$w_{b, i} \cdot w_{b, i}^{-1} \equiv 1 \pmod{b_{i+1}} \dots (12)$$

【0032】

エンティティBにおける復号器5での復号処理は、以下のように行われる。  
中間復号文 $M_o$ は、下記(13)のように与えられる。

【0033】

【数3】

$$M_0 = m_1' b_1 v_1^{(1_1)} + m_2' b_1 b_2 v_2^{(1_2)} + \dots \\ + m_K' b_1 b_2 \dots b_K v_K^{(1_K)} \dots (13)$$

【0034】

よって、下記(14)に示す逐次復号アルゴリズムによって復号できる。なお、以下において  $b_{K+1}$  は  $m_K' < b_{K+1}$  を満たす乱数であるが、基数としては用いられていない。一般にステップ  $i$  における  $j_i$  に対する乱数項は下記(15)のよう表記している。

【0035】

## 【数4】

## 逐次復号アルゴリズム

ステップ1

$$M_1 = \frac{M_0}{b_1}$$

$$m_1' \equiv M_1 \cdot w_{b,1}^{-1} \pmod{b_2}$$

$$m_1' \equiv J_1 \pmod{J}$$

ステップi (i=2~K-1)

$$M_i = \frac{M_{i-1} - m_{i-1}' v_{i-1}^{(j_{i-1})}}{b_i}$$

$$m_i' \equiv M_i w_{b,i}^{-1} \pmod{b_{i+1}}$$

$$m_i' \equiv J_i \pmod{J}$$

ステップK

$$M_K = \frac{M_{K-1} - m_{K-1}' v_{K-1}^{(j_{K-1})}}{b_K}$$

$$m_K' \equiv M_K w_{b,K}^{-1} \pmod{b_{K+1}}$$

... (14)

$$v^{(j_i)} \dots (15)$$

## 【0036】

図3は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、データベース10に予め格納されている複数の公開鍵から各分割平文について任意の公開鍵を選択する処理と、選択した公開鍵と分割平文とを用いて暗号文を作成する処理とを含むか、または、このように作成された暗号文を上述した逐次復号アルゴリズムに従って復号する処理を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ20は、各エンティティ側に設けられている。

## 【0037】

図3において、コンピュータ20とオンライン接続する記録媒体21は、コンピュータ20の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体21には前述の如きプログラム21a が記録されている。記録媒体21から読み出されたプログラム21a がコンピュータ20を制御することにより、コンピュータ20が暗号文Cを作成するか、または、暗号文Cを元の平文xに復号する。

【0038】

コンピュータ20の内部に設けられた記録媒体22は、内蔵設置される例えばハードディスクドライブまたはROM等を用いてなり、記録媒体22には前述の如きプログラム22a が記録されている。記録媒体22から読み出されたプログラム22a がコンピュータ20を制御することにより、コンピュータ20が暗号文Cを作成するか、または、暗号文Cを元の平文xに復号する。

【0039】

コンピュータ20に設けられたディスクドライブ20a に装填して使用される記録媒体23は、運搬可能な例えば光磁気ディスク、CD-ROMまたはフレキシブルディスク等を用いてなり、記録媒体23には前述の如きプログラム23a が記録されている。記録媒体23から読み出されたプログラム23a がコンピュータ20を制御することにより、コンピュータ20が暗号文Cを作成するか、または、暗号文Cを元の平文xに復号する。

【0040】

以下、本発明による暗号化の数値例について説明する。

各種のパラメータを  $J=2$ ,  $K=8$ ,  $|m_i|=8$ ,  $I=2$  とした場合の数値例を以下に示す。なお、平文  $m_i$  の偶奇により夫々  $c_i^{(0)}$  及び  $c_i^{(1)}$  から選択した公開鍵を  $c_i$  と表記した。なお、以下に示す数値例は、上述した逐次復号アルゴリズムによって容易に復号できる。

【0041】

## 【数5】

$$\begin{aligned}P_1 &= 102910906635900382142873 \\w^{(1)} &= 55053873146549250860534 \\w^{(1)-1} &= 32376670821046102944822 \\P_2 &= 260149294473638018394365993 \\w^{(2)} &= 33326843180657116376300668 \\w^{(2)-1} &= 117709177347082312786555509 \\ \{b_i\} &= (1, 293, 271, 263, 311, \\ &\quad 281, 269, 277, 283) \\ \{v_i^{(0)}\} &= (10685899466744021506, \\ &\quad 66258935077143556, \\ &\quad 194062160104827, \\ &\quad 1074494359574, \\ &\quad 3416007300, \\ &\quad 12107042, \\ &\quad 42345, \\ &\quad 997) \\ \{v_i^{(1)}\} &= (15793957966268463201, \\ &\quad 56556565432113505, \\ &\quad 183882213776184, \\ &\quad 1225119957987, \\ &\quad 2506715466, \\ &\quad 16419381, \\ &\quad 37082, \\ &\quad 997) \\ \{w_{b,i}\} &= \{v_i^{(0)} \bmod b_{i+1}\} = \{v_i^{(1)} \bmod b_{i+1}\} \\ &= (235, 233, 210, 128, \\ &\quad 171, 159, 241, 148)\end{aligned}$$

【0042】

【数6】

$$\{B_i^{(0)(1)}\} = \{w^{(1)} b_1 b_2 \dots b_i v_i^{(0)} \bmod P_1\}$$
$$= (10685899466744021506,$$
$$19413867977603061908,$$
$$15409117698803578281,$$
$$22438653891545886686,$$
$$22185633732513926700,$$
$$22095173575982044358,$$
$$20788051585611427695,$$
$$135577173653246484239,$$
$$38483791518424027121)$$

$$\{B_i^{(1)(1)}\} = \{w^{(1)} b_1 b_2 \dots b_i v_i^{(1)} \bmod P_1\}$$
$$= (15793957966268463201,$$
$$16571073671609256965,$$
$$14600799420470338152,$$
$$25584166606322983143,$$
$$16280138277311048814,$$
$$29965128823802018319,$$
$$18204334133844443542,$$
$$135577173653246484239,$$
$$38483791518424027121)$$

$$\{c_i^{(0)}\} = \{B_i^{(0)(2)}\} = \{w^{(2)} B_i^{(0)(1)} \bmod P_2\}$$
$$= (162773815812901090377734403,$$
$$93025051253032697434809027,$$
$$62205285076317806412521471,$$
$$259428598904157633423079243,$$
$$217251256667441573416357617,$$
$$46733606540159864742867102,$$
$$214784340940908602891069724,$$
$$102147719304960540202300258,$$
$$89882645999923806790330549)$$

【0043】



## 【数7】

$$\begin{aligned} \{c_i^{(1)}\} &= \{B_i^{(1)(2)}\} = \{w^{(2)} B_i^{(1)(1)} \bmod P_2\} \\ &= (191272628640899272049659235, \\ &\quad 249985745113542801003131066, \\ &\quad 201270705789948255796606712, \\ &\quad 46555708184749375635052156, \\ &\quad 246511137861367171102859869, \\ &\quad 250687268105719102100996604, \\ &\quad 49005762685980897895931698, \\ &\quad 102147719304960540202300258, \\ &\quad 89882645999923806790330549) \end{aligned}$$

$$\begin{aligned} \{m_i\} &= (199, 188, 217, 237, 142, 254, 189, 249) \\ \{c_i\} &= (191272628640899272049659235, \\ &\quad 93025051253032697434809027, \\ &\quad 201270705789948255796606712, \\ &\quad 46555708184749375635052156, \\ &\quad 217251256667441573416357617, \\ &\quad 46733606540159864742867102, \\ &\quad 49005762685980897895931698, \\ &\quad 102147719304960540202300258, \\ &\quad 89882645999923806790330549) \end{aligned}$$

$$\begin{aligned} C &= m_1 c_1 + m_2 c_2 + \cdots + m_8 c_8 \\ &= 187678294493876349071512183003 \end{aligned}$$

## 【0044】

次に、公開鍵の可能な組合せ数  $N_B$ ，公開鍵リストのサイズ  $S_c$ ，初回伝送暗号文のレート  $R$  及び定常時の暗号文のレート  $r$ （情報記号数／暗号文長）の数値例について述べる。但し、 $J=2$ ， $K=128$ ， $|m_i|=64$ （ビット）とし、 $b_i = 2^{64} + \delta_i$ （ $2 \leq i \leq K$ ）， $b_1 = 1$ ， $1 \ll \delta_i \ll 2^{64}$  とする。なお、最初の暗号文のみ符号化メッセージを用いる。

## 【0045】

$N_B = J^K = 2^{128} \approx 3.40 \times 10^{38}$  となる。公開鍵のサイズ  $|c_i| = 64 \times 128 = 8192$ （ビット）であるので、 $S_c = 8192 \times 2 \times 128 \approx 2.097$ （Mビット）（26 kバイト）となる。また、最初の暗号文の符号化メッセージ  $m_1'$  のサイズは 64（ビット）であり、 $\log_2 J = \log_2 2 = 1$  である。最初の暗号文のメッセージのサイズ  $|m_i|$  は  $|m_1'| = 64$ （ビット）である。従って、最初の暗号文

のレート  $R$  は、 $R = (63 \times 128) / (8192 + 64 + \log_2 128) = 8064 / 8263 = 0.976$

となる。第 2 回目以降の定常時の暗号文のレート  $r$  は、0.991 で与えられる。

#### 【0046】

ところで、 $J = 4$ 、 $K = 64$  と設定した場合、他が同一の条件であるときには、夫々の値が以下のようになる。

$$N_B = 4^{64} \approx 3.40 \times 10^{38}$$

$$S_C = 4096 \times 2 \times 128 \approx 1.048 \text{ (Mビット)} \quad (131 \text{ kバイト})$$

$$R = 0.968$$

$$r = 0.983$$

#### 【0047】

以下、本発明の安全性について考察する。

法  $P$  を秘密にしても、連続する 3 個の公開鍵  $c_{i-1}$ 、 $c_i$ 、 $c_{i+1}$  が正しく与えられた場合には、特定攻撃（境隆一，村上恭通，笠原正雄：“積和型公開鍵暗号に関する二，三の考察” 信学技報 ISEC99, 1999 に開示の攻撃方法）によって、 $b_i$ 、 $b_{i+1}$ 、 $P$  が露呈し、更に、 $P$  が露呈すると連分数攻撃（H. Kuwakado, H. Tanaka：“The security of the improved knapsack cryptosystem”, IEICE Trans., Fundamental, vol. E81-A, no. 10, pp. 2184-2185, 1998 に開示の攻撃方法）によって、 $v_{i,j} < P^{1/2}$  となる乱数項が露呈する可能性がある。

#### 【0048】

ここで公開鍵  $\{c_i\}$  の位置が正当な受信者（エンティティ B）のみが知る順序でランダムにシャッフルされているとすると、攻撃者は総当たりに連続する 3 個の公開鍵を調べることになる。総当たりの回数は  ${}_K C_2 \cdot 3!$  であり、この中に  $(K-2)$  組の正しい連続鍵  $\{(c_{i-1}, c_i, c_{i+1})\}$  が含まれている。従って正しい連続鍵の 1 組  $(c_{i-1}, c_i, c_{i+1})$  当たりに必要な総当たり攻撃の回数  $N_A$  は、下記 (16) で与えられる。 $N_A$  回の総当たり攻撃を試みた場合に 1 組の正解が期待されるので、このときに仮定される鍵系列の集合を正解集合と呼ぶ。

#### 【0049】

【数8】

$$N_A = \frac{{}_K C_3 \cdot 3!}{K-2} \cdots (16)$$

【0050】

本発明の暗号化方式について、「数論と組み合わせたLLL攻撃（上述の特定攻撃）によって秘密の一部が不完全な形ながら露呈すること」によって、安全性に関する下界を定量化することができる。本発明の安全性が非常に高いことは、次のような4点の根拠に基づいている。

①暗号化鍵の位置がランダムにシャッフルされているために、 $N_A$  通りに得られた解の中から正解を決定することが困難であること。

②上位の  $\{v_{ij}\}$  ,  $\{b_i\}$  等が露呈しても、下位の  $\{v_{ij}\}$  ,  $\{b_i\}$  及び乱数  $w$  は露呈しないこと。

③上位の  $\{v_{ij}\}$  ,  $\{b_i\}$  が露呈しても、正しく順序付けることが困難であること。

④上記パラメータが露呈しても、乱数  $w$  が露呈しないのでメッセージは露呈しないこと。

【0051】

以上のように、本発明の基本の暗号化方式は十分に安全であると考えられるが、多段暗号化を行うことにより、より安全性を高くした方式を構築できる。以下、この多段暗号化について説明する。

【0052】

多段暗号化を行う場合には、基数積  $b_1, b_2 \cdots b_I$  に対し、乱数  $w$  と素数  $P$  との組  $(w, P)$  を  $I$  組選択し、下記 (17-1) , (17-2) ,  $\cdots$  , (17-I) のように  $I$  段にわたって乱数を乗じていくことにより、最終的に得られる  $B_1^{(I)}$  を公開鍵  $c_1$  とする。

$$b_1, b_2 \cdots b_I, w^{(1)} \equiv B_1^{(1)} \pmod{P_1} \cdots (17-1)$$

$$B_1^{(1)}, w^{(2)} \equiv B_1^{(2)} \pmod{P_2} \cdots (17-2)$$

$$B_i^{(i-1)} w^{(i)} \equiv B_i^{(i)} \pmod{P_i} \quad \dots (17-I)$$

【0053】

但し、 $I$  個の素数  $P_1, P_2, \dots, P_I$  については、下記 (18) の条件を満たすものとする。下記 (18) は、復号を補償した上で  $P_i$  が  $P_{i+1}$  より小さいことを意味する。また、これらの素数  $P_1, P_2, \dots, P_I$  は全て秘密にする。

$$P_1 < P_2 < \dots < P_I \quad \dots (18)$$

【0054】

なお、多段数  $I$  を十分に大きくすること ( $I > 2^{1/2} K$ ) により、 $\{b_1, b_2, \dots, b_I\}$  は露呈せず、数論的に安全な公開鍵の集合を構成することが可能である。この理由については後述する。

【0055】

$I$  段の多段暗号化を実施した場合、 $(I+2)$  個の公開鍵の順序が正しく与えられると、上述の特定攻撃により、 $\{b_i\}$  の一部と  $\{P_i\}$  とが露呈する。この場合、正解集合のサイズ、即ち、正しい連続鍵の1組  $(c_{i-I}, \dots, c_i, c_{i+1})$  当たりに必要とされる総当たり攻撃の回数  $N_A$  は、下記 (19) で与えられる。

【0056】

【数9】

$$N_A = \frac{K C_{I+2} \cdot (I+2)!}{K-I-1} \quad \dots (19)$$

【0057】

次に、このような多段暗号化における数値例について説明する。各種のパラメータを  $J=2, K=64, |m_i|=64, I=8$  とした場合における公開鍵の可能な組合せ数  $N_B$ ,  $I$  段の多段暗号化を行った場合の正解集合のサイズ  $N_A$ , 第2回以降の定常時の暗号文のレート  $r$  及び公開鍵リストのサイズ  $S_c$  は以下のようになる。

【0058】

【数10】

$$N_B = 2^{64} \approx 1.84 \times 10^{19}$$

$$N_A = \frac{{}^{64}C_{10} \times 10!}{64-8-1} \approx 1.32 \times 10^{18}$$

$$r = \frac{64 \times 64}{64 \times 64 + 7 \times (64 + 6) + \log_2 64}$$

$$= 0.892$$

$$S_C = 2 \times 70 \times (4096 + 7 \times 70)$$

$$= 587 \text{ kビット} = 73.4 \text{ kバイト}$$

【0059】

次に、情報理論的安全性に関する平文分割数 $K$ と多段暗号化の段数 $I$ との関係について考察する。本発明では、以下に述べるような理由により、 $I > 2^{1/2} K$ を満たすようにする。

【0060】

基数 $\{b_i\}$ の唯一つの要素でも露呈した場合には、本発明の暗号化方式の安全性が損なわれると仮定する。この仮定は、非常に安全側に立った仮定である。

$I$ 個の法 $P_1, P_2, \dots, P_I$ は上記(18)の条件を満たし、 $J=2$ とする。また、符号化メッセージ長を $|m'|$ とし、各 $P_i$ のサイズを $|P_i|$ とする。この場合に下記(20)が成り立つ。

【0061】

【数11】

$$|P_I| = |P_1| + (I-1)|m'| + \log_2 K$$

$$\dots (20)$$

【0062】

各公開鍵のサイズを等しく $|c_i|$ とした場合、これらは全部で $JK = 2K$ 個公開されているので、それらを全て合わせたサイズは、 $\log_2 K$ を無視すると、下記(21)のようになる。

【0063】

【数12】

$$\begin{aligned}
 2K|c_1| &= 2K|P_I| \\
 &= 2[K|m'| + (I-1)|m'|]K \cdots (21)
 \end{aligned}$$

【0064】

一方、未知の量としての  $P_1 \sim P_I$  及び  $w^{(1)} \sim w^{(I)}$  までのサイズの和は、下記 (22) のようになる。

【0065】

【数13】

$$\begin{aligned}
 &|P_1| + |P_2| + \cdots + |P_I| \\
 &+ |w^{(1)}| + |w^{(2)}| + \cdots + |w^{(I)}| \\
 &= 2[IK|m'| + \frac{(I-1)I}{2}|m'|] \cdots (22)
 \end{aligned}$$

【0066】

従って、下記 (23) 即ち下記 (24) の条件を満たすように  $I$  を設定した場合には、公開情報量よりも未知情報量が大きくなり、解読が不可能であることは明らかである。この下記 (24) の条件は、近似的に  $I > 2^{1/2} K$  である。

【0067】

【数14】

$$\begin{aligned}
 &2[IK|m'| + \frac{(I-1)I}{2}|m'|] \\
 &> 2[K|m'| + (I-1)|m'|]K \cdots (23)
 \end{aligned}$$

$$(I-1)I > 2(K^2 - K) \cdots (24)$$

【0068】

よって、平文分割数  $K$  と多段暗号化の段数  $I$  との間に  $I > 2^{1/2} K$  の関係がある場合に、 $\{P_i\}$ 、 $\{w^{(i)}\}$  は露呈されず、 $\{b_1, b_2, \cdots, b_i, v_i\}$  が完全に秘匿されるので、極めて安全性が高い。

## 【0069】

また、 $I > K$ である場合、 $\{P_i\}$ 、 $\{w^{(i)}\}$ 、 $\{v^{(i)}\}$ の全てが露呈することはないことを全く同様に示すことができる。

## 【0070】

以下、中国人の剰余定理を応用した本発明の変形方式について説明する。ここでは記号の煩雑さを避けるために、 $P$ に関連する基数を $b_i'$ と表記する。クラス $i$ に属する基数積と乱数項との積の1組を $B_i^{(j)} = b_1 b_2 \dots b_i^{(j)} v_i^{(j)}$ 、 $B_i^{(j)'} = b_1' b_2' \dots b_i^{(j)'} v_i^{(j)'}$ とする。素数 $P$ による余りが $B_i^{(j)}$ 、素数 $Q$ による余りが $B_i^{(j)'}$ となるような最小の整数を $D_i^{(j)}$ とする。更に、 $D_i^{(j)}$ を乱数 $w$ によって下記(25)のように変換し、 $\{c_i^{(j)}\}$ をクラス $i$ の公開鍵として公開する。

$$D_i^{(j)} w \equiv c_i^{(j)} \pmod{PQ} \quad \dots (25)$$

## 【0071】

中間復号文 $M_P$ 、 $M_Q$ は、下記(26)、(27)のようになる。但し、メッセージ $m_i$ はクラス $i$ の何れの公開鍵を用いて暗号化したかを示すために、上式に見られるように $m_i'$ に符号化しているものとする。このような中間復号文 $M_P$ におけるメッセージ $\{m_i\}$ 、中間復号文 $M_Q$ におけるメッセージ $\{m_i'\}$ の復号法は、前述した基本方式の逐次復号アルゴリズムと同様である。

## 【0072】

## 【数15】

$$M_P = m_1' B_1^{(1_1)} + m_2' B_2^{(1_2)} + \dots + m_K' B_K^{(1_K)} \quad \dots (26)$$

$$M_Q = m_1' B_1^{(1_1)'} + m_2' B_2^{(1_2)'} + \dots + m_K' B_K^{(1_K)'} \quad \dots (27)$$

## 【0073】

## 【発明の効果】

以上詳述したように、本発明では、各分割平文毎に設定した乱数項を組み込ん

だ複数の公開鍵を予め準備しておき、準備されているそれらの複数の公開鍵から任意の公開鍵を各分割平文について選択し、選択した公開鍵を使用して暗号文を作成するようにしたので、その公開鍵の選択のパターンが攻撃者には不明であって、攻撃を受けにくく、安全性を向上することができる。従来の公開鍵暗号方式とは異なり、本発明ではその安全性の根拠を、多数の公開鍵から所望の公開鍵の組を自由に選択できること、言い換えれば、その公開鍵選択の組合せの数の多さに置いており、公開鍵暗号方式の発展及び実用化を図る上で、本発明は大いに寄与できる。

## 【００７４】

（付記）

なお、以上の説明に対して更に以下の項を開示する。

- （１） 請求項１記載の暗号化方法であって、前記分割平文と選択した公開鍵とによる複数の積を加算した形式で暗号文を作成する暗号化方法。
- （２） 暗号化すべき平文を分割した分割平文と公開鍵とを用い、前記公開鍵に複数の乱数を多段化演算した演算結果を利用して積和型の暗号文を作成する暗号化方法において、前記平文の分割数 $K$ と前記多段化演算の段数 $I$ とに関して $I > 2^{1/2} K$ の関係を満たす暗号化方法。
- （３） 複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項１または第（１）、（２）項の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文から元の平文を復号する復号器とを備える暗号通信システム。
- （４） コンピュータに、暗号化すべき平文を分割した分割平文と公開鍵とを用いて暗号文を作成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、前記分割平文毎に設定された乱数項が組み込まれた複数の公開鍵から各分割平文について任意の公開鍵を選択することをコンピュータに実行させるプログラムコード手段と、選択した公開鍵を使用して暗号文を作成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されている記録媒体。



整理番号 = 20565

(5) コンピュータに、平文を分割した分割平文と前記分割平文毎に設定された乱数項が組み込まれた複数の公開鍵から各分割平文について選択した公開鍵とを用いて作成された暗号文を復号させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体であって、選択された前記公開鍵を同定しながら前記分割平文を順次復号することをコンピュータに実行させるプログラムコード手段を含むプログラムが記録されている記録媒体。

**【図面の簡単な説明】****【図 1】**

2 人のエンティティ間における情報の暗号通信状態を示す模式図である。

**【図 2】**

データベース内の公開鍵リストを示す図である。

**【図 3】**

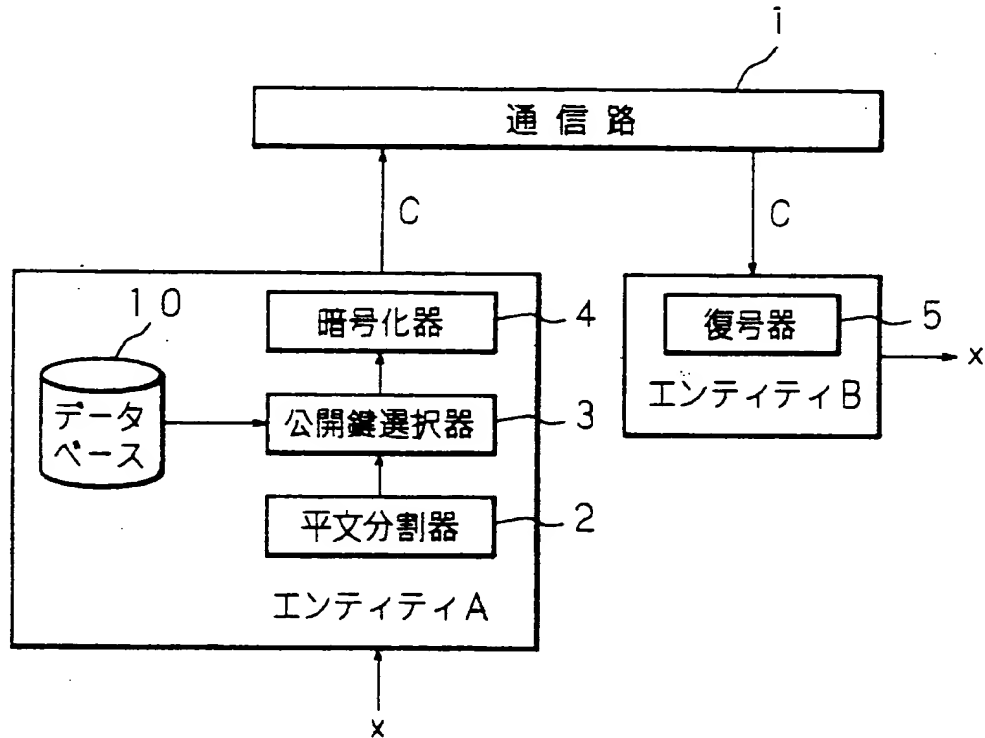
記録媒体の実施の形態の構成を示す図である。

**【符号の説明】**

- 1 通信路
- 2 平文分割器
- 3 公開鍵選択器
- 4 暗号化器
- 5 復号器
- 10 データベース
- 20 コンピュータ
- 21, 22, 23 記録媒体
- A, B エンティティ

【書類名】 図面

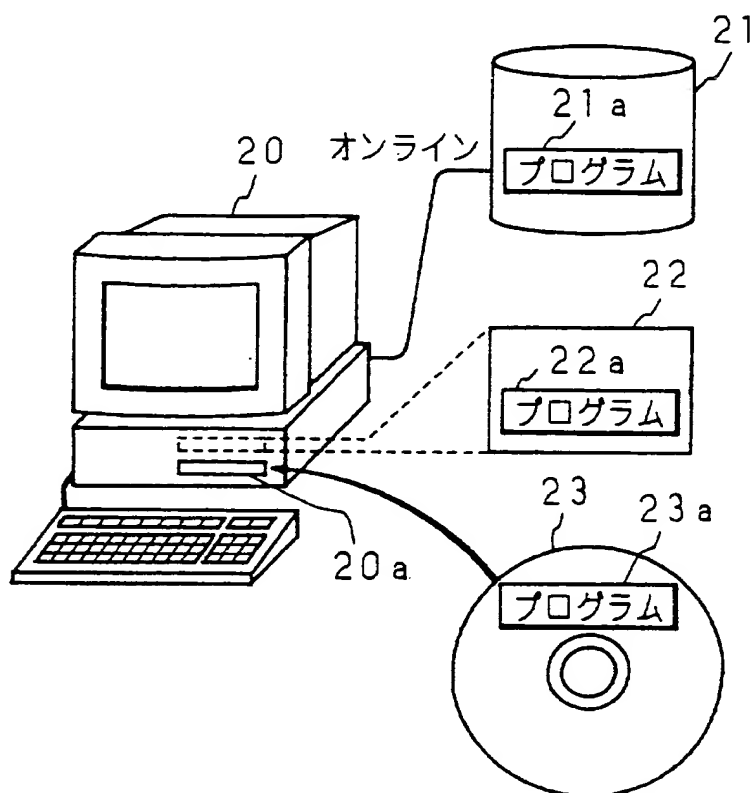
【図1】



【図2】

クラス1	クラス2	...	クラスK
$b_1 v_1^{(1)}$	$b_1 b_2 v_2^{(1)}$	...	$b_1 b_2 \dots b_K v_K^{(1)}$
$b_1 v_1^{(2)}$	$b_1 b_2 v_2^{(2)}$	...	$b_1 b_2 \dots b_K v_K^{(2)}$
$\vdots$	$\vdots$		$\vdots$
$b_1 v_1^{(J)}$	$b_1 b_2 v_2^{(J)}$	...	$b_1 b_2 \dots b_K v_K^{(J)}$

【図3】



【書類名】 要約書

【要約】

【課題】 圧倒的多数の公開鍵の組合せから1つの公開鍵の組を任意に選択することに安全性の根拠を置いた新しいタイプの公開鍵暗号系の暗号化方法を提供する。

【解決手段】 各分割平文毎に乱数項を組み込んだ複数の公開鍵を予めデータベース10内に準備しておき、準備されているそれらの複数の公開鍵から任意の公開鍵を各分割平文について選択し、選択した公開鍵を使用して暗号文Cを作成する。安全性の根拠を、多数の公開鍵から所望の公開鍵の組を自由に選択できること、言い換えれば、その公開鍵選択の組合せの数の多さに置いている。

【選択図】 図1

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**